



A Goal based methodology for HAZOP analysis

Rossing, Netta Liin; Lind, Morten; Jensen, Niels; Jørgensen, Sten Bay

Published in:
International journal of nuclear safety and simulation

Publication date:
2010

[Link back to DTU Orbit](#)

Citation (APA):
Rossing, N. L., Lind, M., Jensen, N., & Jørgensen, S. B. (2010). A Goal based methodology for HAZOP analysis. *International journal of nuclear safety and simulation*, 1(2), 134-142.
<http://www.ijnsweb.com/?type=subscriber&action=journalinfo&effect=&id=2>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

A goal based methodology for HAZOP analysis

ROSSING Netta Liin¹, LIND Morten², JENSEN Niels³, and
JØRGENSEN Sten Bay⁴

1. FLSmith, Vigerslev Allé 77, Valby, Denmark (nr@flsmith.com)

2. Department of Electrical Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark (mli@elektro.dtu.dk)

3. Safepark Consultancy, Kannikestræde 14, DK-3550 Slangerup, Denmark (niels.jensen@safepark.dk)

4. CAPEC, Chemical and Biochemical Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark (sbj@kt.dtu.dk)

Abstract: This paper presents a goal based methodology for HAZOP studies in which a functional model of the plant is used to assist in a functional decomposition of the plant starting from the purpose of the plant and continuing down to the function of a single node, e.g. a pipe section. This approach leads to nodes with simple functions such as liquid transport, gas transport, liquid storage, gas-liquid contacting etc. From the functions of the nodes the selection of relevant process variables and deviation variables follows directly. The knowledge required to perform the pre-meeting HAZOP task of dividing the plant along functional lines is that of chemical unit operations and transport processes plus a some familiarity with the plant a hand. Thus the preparatory work may be performed by a chemical engineer with just an introductory course in risk assessment. The goal based methodology lends itself directly for implementation into a computer aided reasoning tool for HAZOP studies to perform root cause and consequence analysis. Such a tool will facilitate finding causes far away from the site of the deviation. A Functional HAZOP Assistant is proposed and investigated in a HAZOP study of an industrial scale Indirect Vapour Recompression Distillation pilot Plant (IVaRDIP) at the DTU-Dept. of Chemical and Biochemical Engineering. The study shows that the goal based methodology using a functional approach provides a very efficient paradigm for facilitating HAZOP studies and for enabling reasoning to reveal potential hazards in safety critical operations.

Keyword: risk Assessment, HAZOP, multilevel flow modelling

1 Introduction

Hazard analysis provides a systematic methodology for identification, evaluation and mitigation of potential process hazards which can cause serious human, environmental and economic losses. Different methods are practiced at various stages during the plant life cycle. Most methods require considerable time and resources. Consequentially research has been stimulated to develop computer aided tools to assist in or even aiming at automating hazard analysis.

Venkatasubramanian et.al.^[1] reviewed development of knowledge based systems for automating HAZard and OPerability (HAZOP) analysis. Venkatasubramanian and Vaidhyanathan^[2] describe a knowledge based framework, which addresses the representation of process specific and generic knowledge in the automation of HAZOP studies. The generic HAZOP knowledge, which is applicable to a wide variety of flow sheets, is called process general knowledge, while

the remaining HAZOP knowledge is considered specific to a particular process, and is called process specific knowledge. Bragatto et.al.^[3] build upon the notions introduced above and exploits process knowledge with the aim to develop tools for the experts to reveal potential hazards, rooted in a function based taxonomy for equipment and instrumentation. Thus their system includes a dictionary, a plant information database, a reasoning and analysis engine and a knowledge repository. The dictionary permits linking between the terminology used in hazard analysis and a particular application area. In their system objects are categorized according to a hierarchically organised functionality based taxonomy, which can be mapped to the corresponding STEP data definition^[4]. Thus each item is classified in terms of super-function, function type and with an associated set of functional parameters. However the above methods relate the concept of function directly to a physical implementation and therefore they limit the possibility to abstract from one layer in a goal hierarchy to another. Consequently it is desirable to develop a HAZOP analysis methodology based upon a model

Received date: February 16, 2010

representation which can encompass the operational goal hierarchy for the plant. Such a functional model should represent the system using the means-end concepts, where a system is described using goals and purposes in one dimension, and whole-part concepts in another dimension. Such a functional modeling approach lends itself directly for implementation into a computer aided reasoning tool for HAZOP studies to perform cause and consequence analysis. Thereby functional modelling can provide a systematic methodology for computer assisted HAZOP studies, thus potentially relieving the engineers from a major part of a rather cumbersome task and instead permitting them to focus attention where significant problems may be uncovered.

The purpose of this paper is to present the background for development of a functional model based reasoning system for assisting in a goal based methodology for HAZOP analysis. The resulting tool is called a Functional HAZOP Assistant. This tool will be illustrated on an Indirect Vapour Recompression Distillation Pilot Plant (IVaRDIP) located at the Department of Chemical Engineering, at the Technical University of Denmark. The following section briefly introduces a traditional HAZOP, then the functional modeling methodology and the associated reasoning engine are described. The goal based HAZOP analysis methodology using a functional model leads to the Functional HAZOP Assistant, which is presented next. The Functional HAZOP Assistant is demonstrated on the case study. Finally the presented methodology is discussed and the conclusions are drawn.

2 Methods

The proposed methodology is based upon experiences from traditional HAZOP studies. The procedure for such studies is described before introducing a functional modeling paradigm and a workbench for model building and a reasoning engine.

2.1 Traditional HAZOP procedure

Since the development of hazard and operability (HAZOP) studies by Imperial Chemical Industries (ICI) Ltd. in the mid 1960's these have been a cornerstone in risk assessment of process plants^[5-7]. The purpose of the HAZOP study is to investigate how a facility

responds to deviations from design intent or from normal operation, i.e. to reveal if the plant has sufficient control and safety features to ensure, that it can cope with expected deviations normally encountered during operation. The HAZOP study is traditionally performed as a structured brainstorming exercise facilitated by a HAZOP study leader and exploiting experience of the participants. A traditional HAZOP study has the following phases^[8]:

- **Pre-meeting phase:** The purpose and objective of the study is defined. The leader of the HAZOP study gathers information about the facility, such as process flow diagrams (PFD), piping & instrumentation diagrams (P&ID), a plant layout, chemical hazard data etc., and proposes a division of the plant into sections and nodes. For each node - or for the plant as a whole - the leader identifies relevant process variables and deviations from design intent or normal operation based on either past experience or company guidelines. The leader also identifies the participants, who will participate in the review of the different sections of the plant, and ensures their availability. Typically this group includes the process design engineer, the control engineer, the project engineer and an operator besides the experienced team leader. All these people have large demands on their time during a project. The team leader schedules a sufficient number of half day HAZOP meetings.
- **Meeting phase:** At the start of the HAZOP meeting the technique is briefly reviewed, and the specific scope of the present study is stated. The overall facilities are described e.g. using a 3D computer model. Then the team considers each P&ID or PFD in turn. The team leader ensures that process variables and deviations are considered in a rigorous and structured manner, that results are recorded, and that all areas meriting further consideration are identified by action items.
- **Post-meeting phase:** After the HAZOP meeting all actions items are followed up by the persons assigned to them during the meeting and the results of the follow-up is reported to the team leader. The team might call a review meeting to determine the status of all actions items, and decide if additional efforts are needed.

Thus a HAZOP study requires considerable time and

resources whenever it is carried out during the plant life cycle. Consequentially research has been stimulated to develop computer aided tools to assist in or even aiming at automating hazard analysis and especially HAZOP studies.

Although HAZOP analysis is a well accepted tool for risk assessment in many industries very little has been published on a theoretical basis for HAZOP studies. HAZOP studies are used to investigate deviations from a norm: the normal operating conditions or the design intent, i.e. the goal of the system. This is traditionally done by asking questions such as what deviations can occur? Why do they occur? (causes), How are they revealed? (consequences). These questions are asked after first dividing the whole system into its constituent parts. The questions stated relate to the goal of the system while the process represents the means for achieving these goals. Therefore it seems highly relevant to develop a HAZOP assistant based upon means-ends modelling combined with whole-parts concepts to grasp the different levels of abstraction when needed. Thus models based on these concepts, such as functional models will form a convenient basis for an HAZOP assistant. The HAZOP assistant developed in this work uses a functional model to combine the system goal structure with the means to achieve these goals.

In the following section a HAZOP assistant using a functional model builder to build a MFM model of the system and a reasoning engine are presented before the goal based methodology for HAZOP analysis using a functional approach is proposed.

2.2 Functional modelling methodology

Multilevel Flow Modeling (MFM) is used here to combine the means-end dimension with the whole part dimension, to describe the functions of the process under study and to enable modelling at different abstraction levels. MFM is a modeling methodology which has been developed to support functional modeling of process plants involving interactions between material, energy and information flows[9],[10]. Functions are here represented by elementary flow functions interconnected to form flow structures representing a particular goal oriented view

of the system. MFM is founded on fundamental concepts of action developed by VonWright^[11]. Each of the elementary flow functions can thus be seen as instances of more generic action types. The views represented by the flow structures are related by means-end relations and comprise together a comprehensive model of the functional organization of the system. The basic modeling concepts of MFM comprises objectives, flow structures, a set of functional primitives (the flow functions) and a set of means-end relations and causal roles representing purpose related dependencies between functions. The functions, the flow structures and the relations are interconnected to form a hypergraph like structure.

2.3 Functional model builder and reasoning system

A MFM model builder has been developed in MSVisio. Stencils implementing icons for the MFM concepts are used to build a model graphically, see Fig 1. The model builder is interfaced with a reasoning system which can generate root causes and causal paths for a given fault scenario i.e. a top event (failed MFM function) and status information for selected flow functions. The reasoning system is implemented using the Java based expert system shell Jess^[12]. Rules for reasoning about function states in MFM models are implemented as a Jess rule base.

The MFM-models consist of flow function blocks, causal roles and flow structures, as shown in Fig 2. The current set of function blocks are source, transport, balance and sink. Definition of the causal roles is essential as they enable implementation of a reasoning system. Work is presently on going to extend the set of functions to easier handle chemical reactions and multicomponent systems.

3 Results

The functional modeling approach described above forms the basis for a developing a functional HAZOP assistant for a goal based methodology for HAZOP analysis.

3.1 A Functional HAZOP assistant

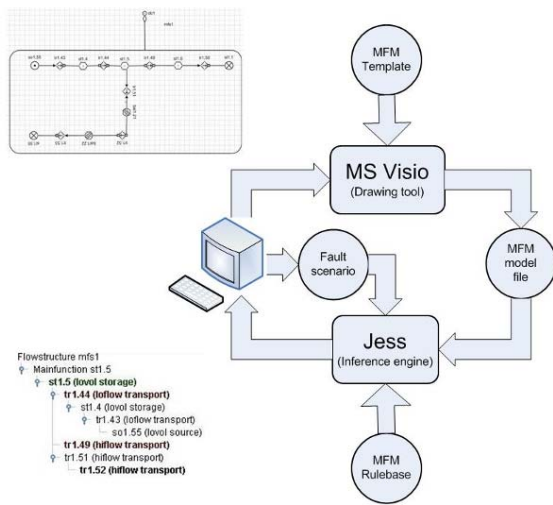


Fig 1. MFM model builder and reasoning system.

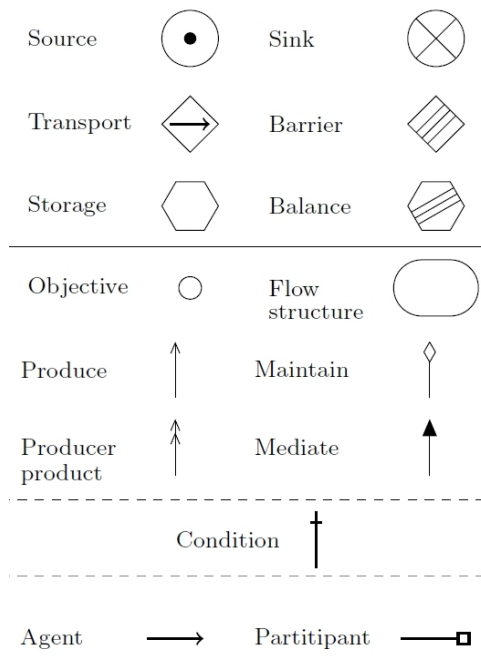


Fig 2. Elements of MFM models consist of flow functions (row one and two) and causal roles (row three).functions (row one and two) and causal roles (row three).

Traditionally the division of the plant into sections may be done by defining each major process component as a section. A section could also be a line between each major component with additional sections for each branch of the main process flow direction. Usually the function of a section or of a node is not directly specified; many HAZOP formats only identify the part of the process considered by project number, P&ID number and line number. The design intent of the node may go unrecorded, even though the purpose of the

HAZOP study is to consider deviations from design intent.

The goal based methodology for HAZOP analysis provides a structured approach where the study is divided into three phases, corresponding to the traditional approach described above. The first phase corresponds to the premeeting phase, the second phase to the meeting phase and the third phase to the post meeting phase. Thus the Functional HAZOP assistant involves the following steps^[13]:

Phase 1:

1. State the purpose of the plant.
2. Divide the plant into sections each of which has a clear sub-purpose or -aim in contributing to the overall purpose of the plant.
3. Divide each section into nodes, the function of which can be directly described by physical or chemical phenomena. Examples of such phenomena are: gas transport, liquid transport, liquid storage and gas-liquid contact.
4. At this point an MFM model may be directly developed using the model builder as described above (in case a model is not already available) provided that the physical and chemical phenomena are included in the existing model set.
5. For each type of node, i.e. each physical or chemical phenomenon, describe the process variable(-s), which identifies design intent or normal operation. For a node with the function 'gas transport' normal operation could be described by flow rate, temperature, pressure and number of phases.
6. For each process variable specify the relevant deviations. For flows relevant deviations could be more, less and reverse. In this work the deviation 'no flow' is considered a limiting situation of 'less flow', and hence is not considered separately.

Phase 2:

1. Perform the diagnosis on the MFM workbench by working through the plant sections and nodes in sequence and analysing the deviations one by one.
2. Analyse the identified causes of hazardous conditions perhaps by refining the analysis through a more detailed study in case of a serious hazard or cause.

- Record the identified causes and the underlying reasoning for later reference.

Phase 3:

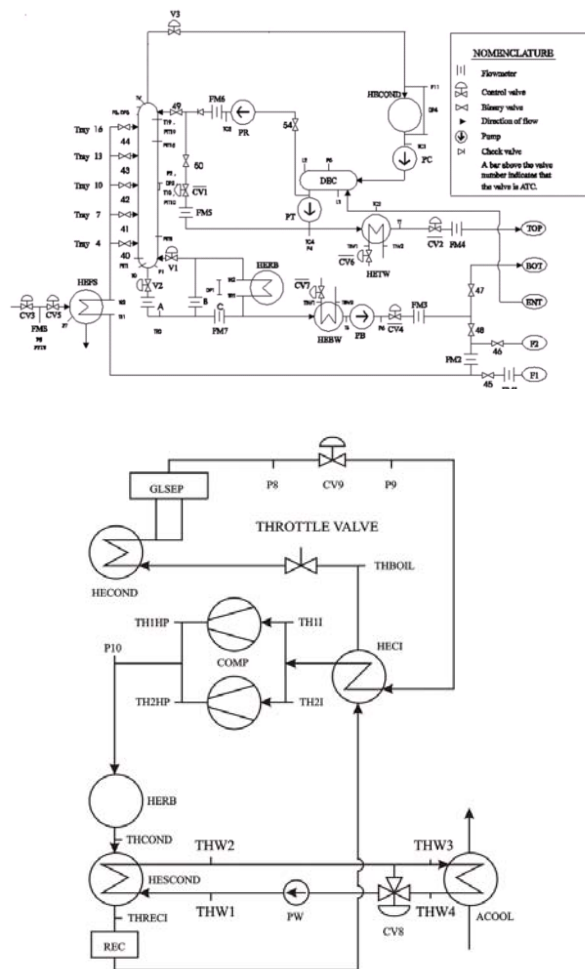
- For identified hazards then investigate and decide how to manage these, through a) definition of an alarm with a consequential response potential for the operator, b) Implementation of modified on line control of the plant, c) redesign of a part of the plant, or d) another action.
- Record the final decision and the underlying reasoning for later reference.

Phase 1 may be carried out in a straightforward manner by using the functional approach. For example the aim of the plant could be to produce 50 tons of PE per hour. In order to achieve this we need sections which: feed reactants to the reactor, feed catalyst to the reactor, reaction, remove excess heat from the reactor, remove product from the reactor, remove of unreacted hydrocarbons from product, add additives to virgin PE etc. The reaction section could be considered as a single node with the purpose of providing suitable conditions, such that raw materials react to form products. For a Unipol PE reactor this would require maintaining fluidization of the PE particles to facilitate their growth as well as the transport of heat of reaction away from the PE particles to ensure they do not melt or fuse together.

Using this approach to dividing the plant all that is needed is a basic understanding of chemical unit operations, their purposes and the fundamentals on which these purposes are built, i.e. transport phenomena. This means that phase 1 of a HAZOP study may be efficiently performed by less experienced personnel. Phase 2 requires more experience.

The above proposed three step procedure clearly becomes a significant task even though the HAZOP assistant will enable consistent reasoning not only within the single nodes but also between nodes and sections and thereby facilitate revealing more complex causes of deviations than possible using the traditional approach. The workflow during phase 2 would indeed be expected to be significantly facilitated though the HAZOP assistant. During phase three the functional modelling may actually also be utilized. However, this has not been studied in the present work.

The application of the Functional HAZOP assistant is



defined:

- **Column section.** Purpose: Gas-liquid contact to facilitate separation.
- **Re-flux section.** Purpose: Provide a liquid stream to the column and remove excess liquid as top product.
- **Feed section.** Purpose: Provide a feed stream as close as possible to the conditions on the feed plate.
- **Re-boiler section.** Purpose: Provide a gas stream to the column and remove excess liquid as bottoms product.
- **Low pressure heat pump section.** Purpose: Transport energy from re-flux section to compressors.
- **High pressure heat pump section, including compressors.** Purpose: Increase the heat pump fluid energy content by compression and transport heatpump fluid from compressors to re-boiler.
- **Excess heat removal section.** Purpose: Transport of excess energy from the heat pump to the environment.
- **Tank Park.** Purpose: Provide storage for raw material and products.

3.3 Building an MFM model

The IVaRDIP is divided into 8 sections in step 2 of the functional HAZOP approach. Then each section is further divided into nodes according to their function. For example the re-flux section, see Fig 3, which consists of the piping from the top of the column through the condenser and accumulator (DEC) back to the column as well as the piping from the accumulator to the top product storage tank, is divided into the following nodes during step 3:

- **Node 1.** Function: Gas transport. Piping from the column to the condenser (HECOND) including the emergency shutdown valve (V3) and other instrumentation.
- **Node 2.** Function: Liquid transport. Condenser and piping from condenser to accumulator including a pump (PC) and other instrumentation.
- **Node 3.** Function: Liquid storage. Accumulator (DEC) and associated instrumentation.

- **Node 4.** Function: Liquid transport. Piping from accumulator to top product storage including the product pump (PT) and product cooler (HETW) with the associated instrumentation.
- **Node 5.** Function: Liquid transport. Piping from the accumulator to the column, where re-flux enters, including the re-flux pump (PR) and associated instrumentation.

Upon this subdivision of the section it is directly possible to construct the MFM using the MFM workbench described above. The MFM-model of the reflux section is shown in Fig 5 using the symbols shown in Fig 2. The model begins with the source of gas from the column, which is represented by the source function so1.55. The source function is connected to a transport function tr1.43, which represents the transport of gas from the column to the condenser, HECOND – see Fig 3. The condenser is represented by the storage function st1.4. Following the condenser the liquid moves to the reflux drum (DEC in Fig 3), and this transport, which in the physical plant is performed by pump PC (see Fig 3) is represented by the flow function tr1.44, while the reflux drum is represented by the storage function st1.5. From the reflux drum the liquid can move either back to the column as reflux or to the top product tank as product.

The path from the reflux drum to the product tank is modelled by 4 flow functions: the transport function tr1.49, which represents the top product pump, the storage function st1.6, which represents the top product cooler HETW (see Fig 3), the transport function tr1.50, which represents a control valve, and the sink function si1.1, which represents the top product storage tank.

The path from the reflux drum and back to the column as reflux is modelled by 6 flow functions: the transport function tr1.51, which represents a binary valve, the balance function bal1.21, which represents a section of pipe, the transport function tr1.52, which represents the reflux pump PR (see Fig 3), the balance function bal1.22, which represents another section of pipe, the transport function tr1.53, which represents another

valve, and finally the sink si1.55, which represents the column. Note this model could be simplified, e.g. by combining the transport function tr1.51, the balance function bal1.21 and the transport function tr1.52 into a single transport function. Likewise additional detail could be added to parts of the model as needed given the purpose of the MFM modelling. Rossing^[13] expands on the model of reflux section, and derives a model of the complete IvaRDiP pilot plant, as shown in Fig 7.

The other sections of the distillation pilot plant are similarly divided into nodes, i.e. each node relates to a function described by physical or chemical phenomena. In this way a total of 20 nodes are defined. However, several nodes have the same function, as can already be seen from the above sub-division of the re-flux section. In fact 7 of the 20 nodes have the function 'liquid transport'. Having developed the MFM model for the different nodes these are directly concatenated to form the MFM model for the plant. In defining the function of the node the variables necessary to describe design intent follows directly. E.g. the process variables and deviations relevant for the function 'liquid transport' will be:

- Flow: more, less, reverse, as well as.
- Temperature: lower, higher.

and similarly for the function 'gas transport'

- Flow: more, less, reverse, as well as.
- Temperature: lower, higher.
- Pressure: lower, higher

Having completed phase 1 it is now possible to enter phase 2, where the reasoning engine is used to perform the actual HAZOP study in step 7. During this step the HAZOP Assistant can be extremely helpful in providing the reasoning necessary to identify potential hazards. Initially it is recommended to perform the exhaustive evaluation for each variable in each node. Later as experience is accumulated it may be possible to facilitate also this step further. Below two analyses carried out on the IvaRDiP will be described briefly.

As an example of the application of the reasoning engine the causal tree for the deviation: low volume in storage function st1.5 is shown in Fig 6. The reasoning

engine finds, that low volume in the storage function can be caused by low flow towards the storage or high flow from the storage. Rossing^[13] presents more extended reasoning results for different MFM models.

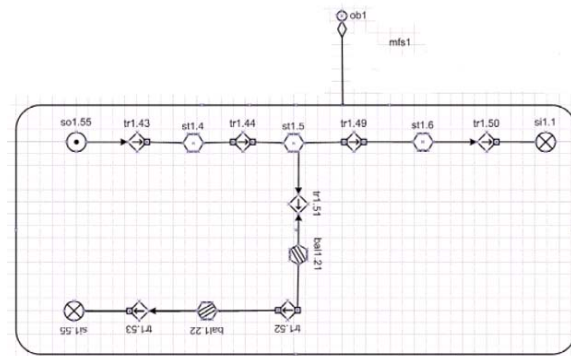


Fig 5. MFM-model of the reflux section of IvaRDiP.

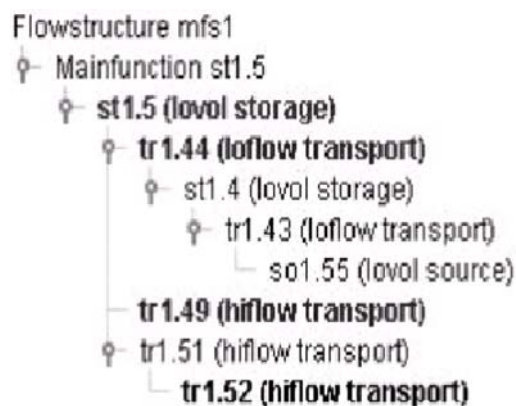


Fig 6. Causal tree of the event low volume in storage function st1.5 obtained by using the reasoning engine on the MFM-model of the reflux section shown in Fig 5.

3.3 Traditional versus functional HAZOP

The result of a traditional HAZOP of the re-flux section of the distillation pilot plant is compared to the results of the Functional HAZOP Assistant. The results demonstrate that while the traditional approach provides 14 records in the HAZOP, then the Functional HAZOP Assistant only provides 8 records with the same information content. Hence the Functional HAZOP Assistant requires half the effort in evaluating the causes of deviations, i.e. the number of lines in the HAZOP report. Clearly the time required to perform the HAZOP will be significant shorter for the HAZOP Assistant, when a MFM model is available, than for a traditional HAZOP.

In addition the availability of a scientifically based systematic approach to performing the HAZOP provides an interesting potential for the HAZOP study to cover the possible hazards in a plant foreseeable with the applied abstraction level in the MFM modelling. However a more detailed and systematic study of the different steps in the three phases of a HAZOP needs to be performed to further validate such a speculation.

3.5 Plant wide HAZOP

The ability of the Functional HAZOP Assistant also has been investigated for revealing more complex hazards in a plant. Here a very simplified functional model was developed for the IVaRDiP as shown in Fig 7, where the mass flow of the distillation column is combined with a very simple energy flowstructure for the heat pump shown in the upper left hand side of the Fig. Using this model it was shown that the Functional HAZOP Assistant facilitates the discovery of root causes of deviations, which originate far from the node in which the deviation occurs. Some recent loss events in the chemical industry have involved such situations^[14].

4 Discussion and conclusions

A goal based methodology for HAZOP analysis using a Functional HAZOP procedure is introduced, which allows even fresh chemical engineers to contribute meaningfully to a HAZOP study. The approach reduces the work involved in a HAZOP of a plant by dividing the plant along functional lines and analysing nodes with the same function once only. This also appears to reduce the needed time commitment of key personnel towards a HAZOP study. Furthermore functional models of chemical plants are demonstrated to provide a useful approach for development of a Functional HAZOP Assistant. On a simple model of a part of an indirect vapour recompression distillation pilot plant the Functional HAZOP Assistant finds the same causes as a traditional HAZOP study. It has furthermore been demonstrated, that the proposed Functional HAZOP Assistant is able to find causes far from the site of the deviation. This promising development calls for a more systematic study of the workflow involved in HAZOP

studies to further enable design of efficient tools for supporting the important HAZOP studies for improvements in Safety Critical Operations of the increasingly complex infrastructures employed in

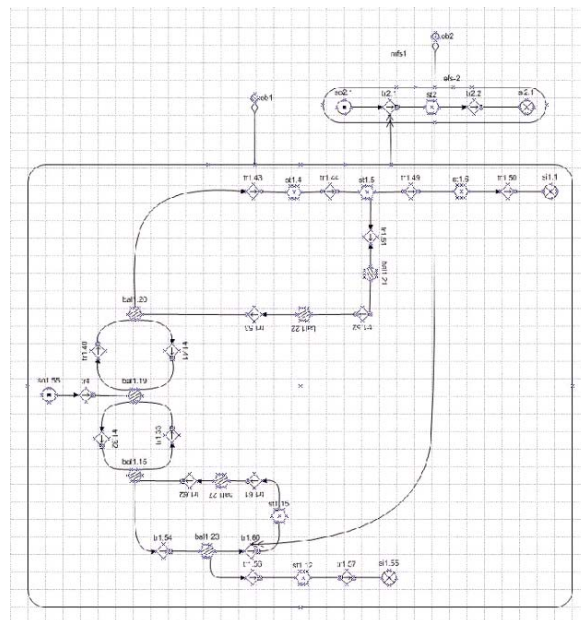


Fig 7. Simple total mass flow MFM model of distillation pilot plant with objectives to maintain constant level in the accumulator and constant energy flow in the heat pump.

society such as power plants using many different power sources: nuclear, hydrocarbons, wind and biofuels.

References

- [1] VENKATSUBRAMANIAN, V., ZHAO, J. VISWA-NATHAN, S.: Intelligent systems for HAZOP analysis of complex process plants, computers chemical engineering, 2000, 24(24):2291-2302.
- [2] VENKATSUBRAMANIAN, V., VAIDHYANATHAN, R.: A knowledge-based framework for automating HAZOP analysis, AIChE J., 1994, 40(3):496-505.
- [3] BRAGOTTO, P., MONTI, M., GIANNINI, F., ANSALDI, S.: Exploiting process plant digital representation for risk analysis, J. LOSS PREV. PROCESS IND., 2007, 20(1):69-78.
- [4] STEP ISO STANDARD 10303-1: Industrial automation systems and integration-product data representation and exchange—Part I: Overview and fundamental principles, 1994.
- [5] CRAWLEY, F., TYLER, B.: Hazard identification methods, Rugby: IChemE, 2003.
- [6] LEES, F.P.: Loss prevention in the process industries,

- Oxford: Butterworth-Heinemann, 2001:3rd edition.
- [7] LAWLEY, H.G.: Operability studies and hazard analysis, Chem. Engng. Progress, 1974 70(4): 45-56.
 - [8] SKELTON, B.: Process safety analysis - an introduction, Rugby: IChemE, 1997.
 - [9] LIND, M.: Representing goals and functions of complex systems. An Introduction to Multilevel Flow Modelling, Kgs.Lyngby: Technical University of Denmark, 1990.
 - [10] LIND, M.: Modeling goals and functions of complex industrial plant, APPL. Artificial Intelligence, 1994 8(2):259-283.
 - [11] VON WRIGHT, G. H.: norm and action, London: Routledge & Kegan, 1963.
 - [12] FRIEDMAN-HILL, E.: Jess in action, Greenwich: Manning Publications, 2003.
 - [13] ROSSING, N.L.: Method development for systematic risk assessment, Kgs.Lyngby: Technical University of Denmark Dept.of Chemical Engineering, M.Sc. Thesis, 2006.
 - [14] MOGFORD, J.: Fatal accident investigation report, Texas City:BP, 2005.